BEZPEČNOSTNÝ BULLETIN

Týždeň 01. 08. 2018 – 07. 08. 2018

OBSAH BEZPEČNOSTNÉHO BULLETINU

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Mozilla Foundation Security Advisory 2018-19

Popis

Spoločnosť Mozilla vydala bezpečnostnú aktualizáciu svojho e-mailového klienta Mozilla Thunderbird, ktorá opravuje viacero bezpečnostných zraniteľností.
Najvážnejšia bezpečnostná zraniteľnosť sa nachádza vo funkcii spracovania grafických polí a umožňuje vzdialenému neautentifikovanému útočníkovi spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

06.08.2018

CVE

CVE-2018-12359, CVE-2018-12360, CVE-2018-12361, CVE-2018-12362, CVE-2018-5156, CVE-2018-12363, CVE-2018-12364, CVE-2018-12365, CVE-2018-12366, CVE-2018-12367, CVE-2018-12371, CVE-2018-12368, CVE-2018-5187, CVE-2018-5188

Zasiahnuté systémy

Mozilla Thunderbird verzie staršie ako 60

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému
Zneprístupnenie služby, Eskalácia privilégií, Neoprávnený prístup k citlivým údajom

Odporúčania

Administrátorom a používateľom zasiahnutých systémov odporúčame nainštalovať bezpečnostné aktualizácie. Taktiež odporúčame poučiť používateľov, aby neotvárali neoverené e-mailové správy a prílohy z neznámych zdrojov.

Zdroje

https://www.mozilla.org/en-US/security/advisories/mfsa2018-19/

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.8**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

WECON LeviStudioU Vulnerabilities

Popis

Spoločnosť WECON Technology Co., Ltd. vydala bezpečnostnú aktualizáciu na svoj produkt LeviStudioU, ktorá opravuje bližšie nešpecifikované bezpečnostné zraniteľnosti.
Bezpečnostné zraniteľnosti sú spôsobené nedostatočným overovaním používateľských vstupov a umožňujú vzdialenému útočníkovi pomocou podvrhnutia špeciálne upravených HSC súborov spôsobiť pretečenie zásobníka a následne vykonať škodlivý kód.

Dátum prvého zverejnenia varovania

31.07.2018 (posledná aktualizácia 01.08.2018)

CVE

CVE-2018-10602, CVE-2018-10606

Zasiahnuté systémy

LeviStudioU verzie 1.8.29 a 1.8.44

Následky

Vykonanie škodlivého kódu a úplné narušenie dôvernosti, integrity a dostupnosti systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov, aplikovať firewallové pravidlá a limitovať prístup k zasiahnutým zariadeniam a jeho funkciám zavedením zoznamu pre riadenie prístupov (ACL).

Zdroje

https://ics-cert.us-cert.gov/advisories/ICSA-18-212-03

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.6**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Drupal Core - 3rd-party libraries -SA-CORE-2018-005

Popis

Vývojári systému pre správu obsahu Drupal vydali aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť v knižniciach Symfony a Zend.
Bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov pri spracovávaní HTTP hlavičiek a umožňuje vzdialenému neautentifikovanému útočníkovi prostredníctvom X-Original-URL a X-Rewrite-URL HTTP požiadaviek získať prístup k citlivým údajom.

Dátum prvého zverejnenia varovania

01.08.2018

CVE

CVE-2018-14773

Zasiahnuté systémy

Drupal 8.x staršie ako verzia 8.5.6
Symfony verzie staršie ako 2.7.49, 2.8.44, 3.3.18, 3.4.14, 4.0.14, a 4.1.3
Zend framework zend-diactoros verzie staršie ako 1.8.4
Zend framework zend-http verzie staršie ako 2.8.1
Zend framework zend-feed verzie staršie ako 2.10.3

Následky

Neoprávnený prístup k citlivým údajom

Odporúčania

Odporúčame uistiť sa, či Vaše webové stránky nie sú založené na systéme pre správu obsahu Drupal v zraniteľných verziách. V prípade, že áno, zabezpečte jeho aktualizáciu.

Zdroje

https://www.drupal.org/SA-CORE-2018-005
https://symfony.com/blog/cve-2018-14773-remove-support-for-legacy-and-risky-http-headers
https://thehackernews.com/2018/08/symfony-drupal-hack.html

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 8.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Cisco Prime Collaboration Provisioning Unauthorized Password Change Denial of Service Vulnerability

Popis

Spoločnosť Cisco vydala bezpečnostnú aktualizáciu na svoj produkt Cisco Prime Collaboration Provisioning, ktorá opravuje bezpečnostnú zraniteľnosť vo funkcii zmeny hesla.

Bezpečnostná zraniteľnosť spočíva v nedostatočnom overovaní používateľských vstupov a umožňuje vzdialenému autentifikovanému útočníkovi zadať pri zmene hesla reťazec nepovolenej dĺžky a tým spôsobiť zneprístupnenie služby.

Dátum prvého zverejnenia varovania

01.08.2018

CVE

CVE-2018-0391

Zasiahnuté systémy

Cisco Prime Collaboration Provisioning (PCP) verzie 12.2 a staršie

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180801-pcp-dos

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Linux Kernel TCP implementation vulnerable to Denial of Service

Popis

Vývojári linuxového jadra vydali bezpečnostnú aktualizáciu svojho produktu, ktorá opravuje bezpečnostnú zraniteľnosť vo funkciách tcp_collapse_ofo_queue() a tcp_prune_ofo_queue().
Bezpečnostná zraniteľnosť umožňuje vzdialenému útočníkovi prostredníctvom zasielania špeciálne upravených TCP paketov spôsobiť zneprístupnenie služby na zasiahnutom systéme.

Dátum prvého zverejnenia varovania

06.08.2018

CVE

CVE-2018-5390

Zasiahnuté systémy

Linux kernel verzie 4.9+

Následky

Zneprístupnenie služby

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://www.kb.cert.org/vuls/id/962459

Dôležitosť	☐ **Nízka**	☐ **Stredná**	☒ **Vysoká**	☐ **Kritická**	**CVSS skóre: 7.1**
Klasifikácia	☒ **Neutajované / TLP (WHITE)**		☐ **Vyhradené**	☐ **Dôverné**	☐ **Tajné**
Kód sektora (dopad)					

Identifikátor

Apache Tomcat Native OCSP Pre-Produced Responses Unauthorized Access Vulnerability

Popis

Vývojári webového servera Apache Tomcat Native vydali aktualizáciu svojho produktu, ktorá rieši viaceré bezpečnostné zraniteľnosti.
Najvážnejšia bezpečnostná zraniteľnosť spočíva v nedostatočnej implementácii bezpečnostných mechanizmov pri spracovaní Online Certificate Status Protocol požiadaviek. Zraniteľnosť umožňuje vzdialenému autentifikovanému útočníkovi získať prostredníctvom revokovaných certifikátov neoprávnený prístup do systému.

Dátum prvého zverejnenia varovania

06.08.2018

CVE

CVE-2018-8020, CVE-2018-8019

Zasiahnuté systémy

Apache Tomcat Native Connector verzie staršie ako 1.2.17

Následky

Neoprávnený prístup do systému

Odporúčania

Administrátorom odporúčame vykonať aktualizáciu zasiahnutých systémov.

Zdroje

https://tools.cisco.com/security/center/viewAlert.x?alertId=58558
http://tomcat.apache.org/security-native.html